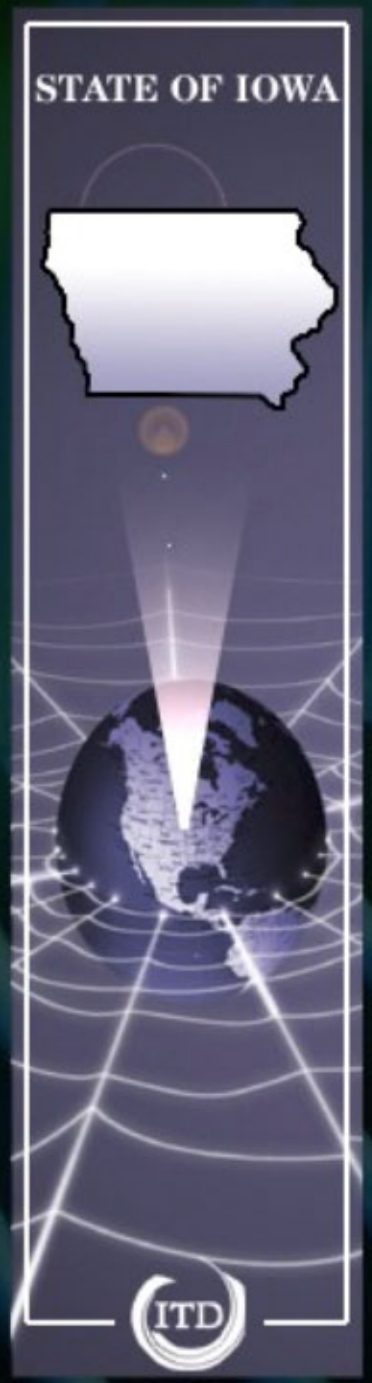
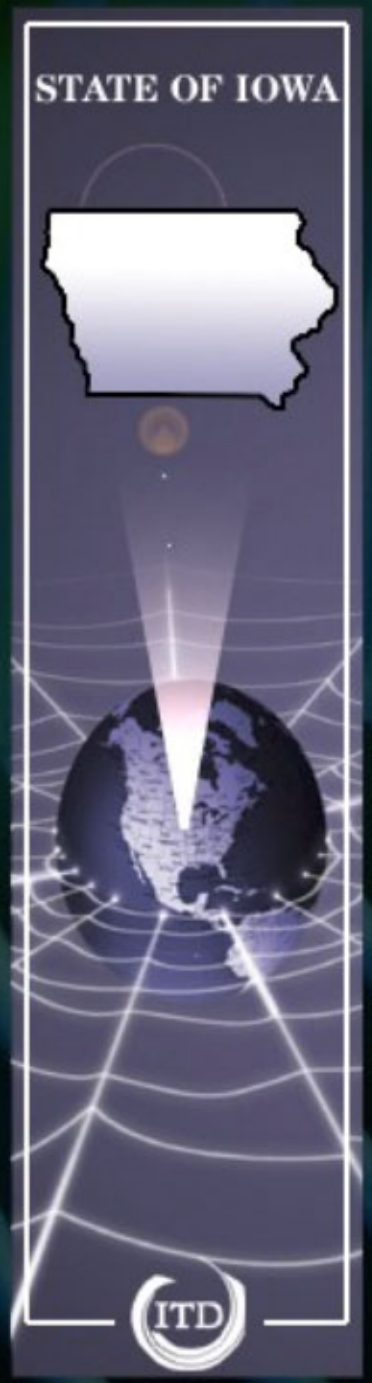


Security and Application Development

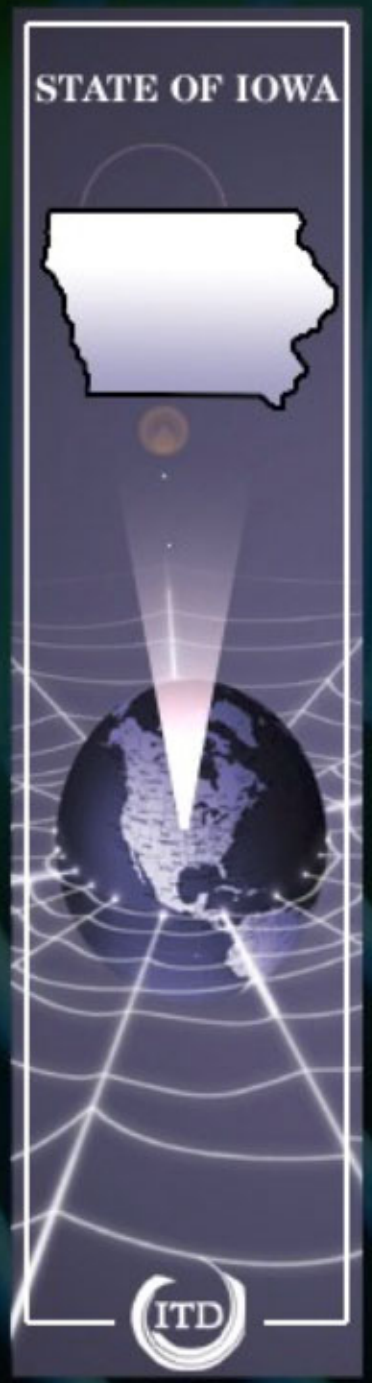
Awareness, Design, and Weakness

March 19, 2002



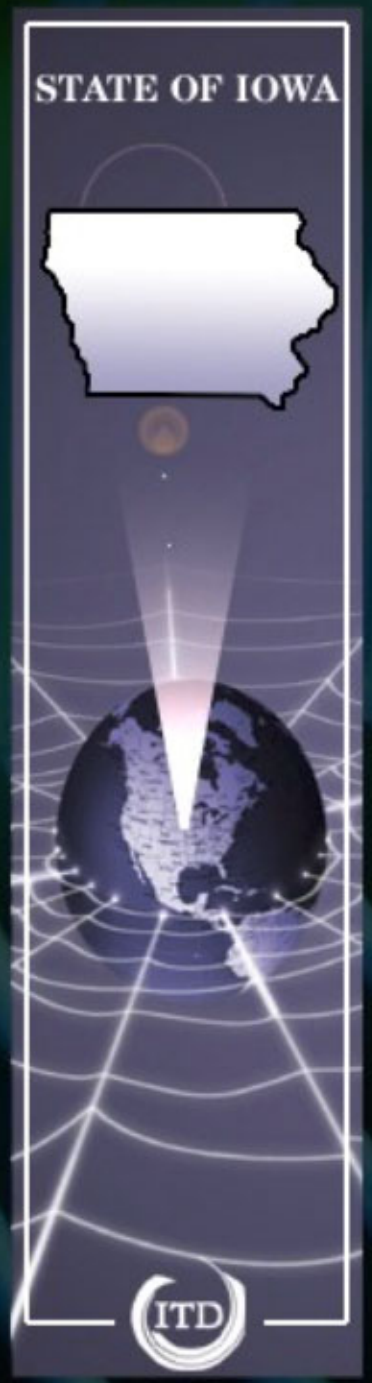
Security Awareness

- Protect State Information Systems and State Assets
- Confidentiality, Integrity, and Accessibility



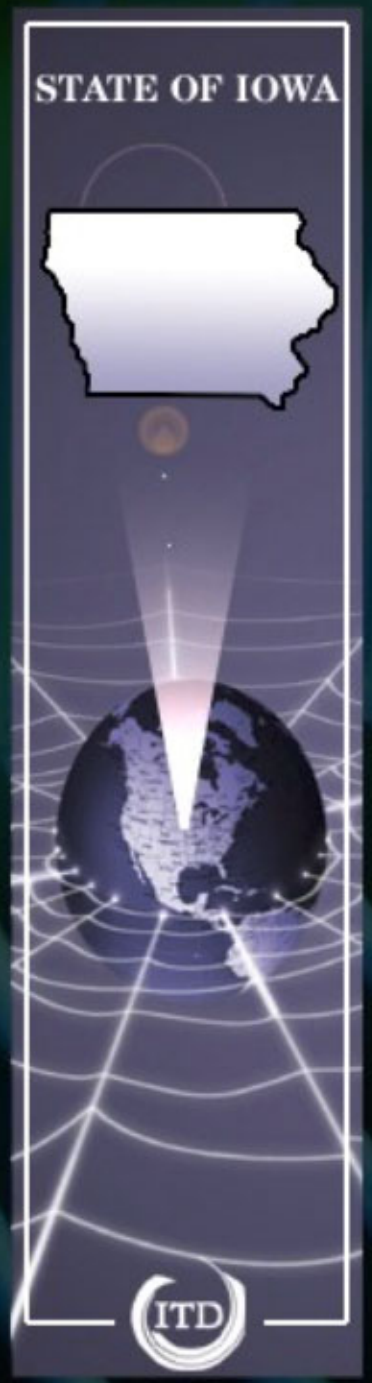
Threats and Awareness

- Criminal Behavior
- Accidents
- Goal is to Limit Potential Breaches of Security



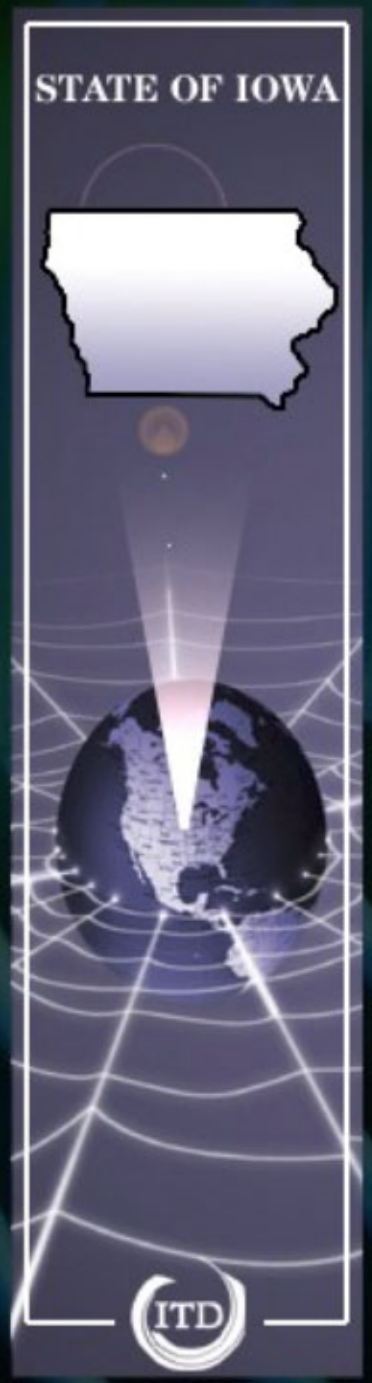
Passwords

- Use Good Passwords
  - 8+ characters
  - Numbers, mixed case letters, and special characters
  - Pass phrase
  - Don’t use names, common words, combinations of words, or easy to guess passwords



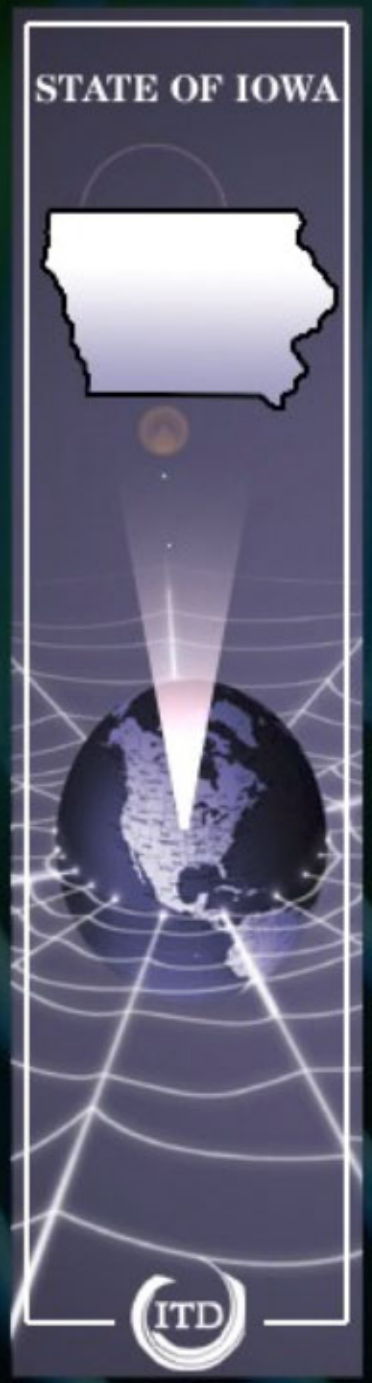
Passwords 2

- Protect Your Passwords
  - Change every 60 days
  - Do not write passwords down
  - Do not store passwords in your computer or online
  - Do not share passwords, change immediately afterwards if you do
  - Do not send passwords via unencrypted e-mail



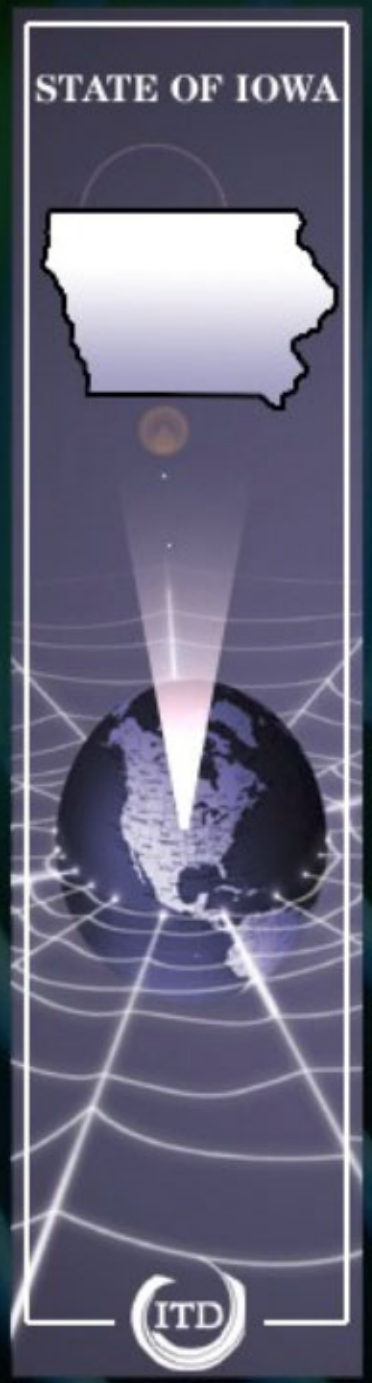
Workstations

- Lock Your Workstation When You Leave It
- Automatic Screen Saver Lock Should Be Enabled



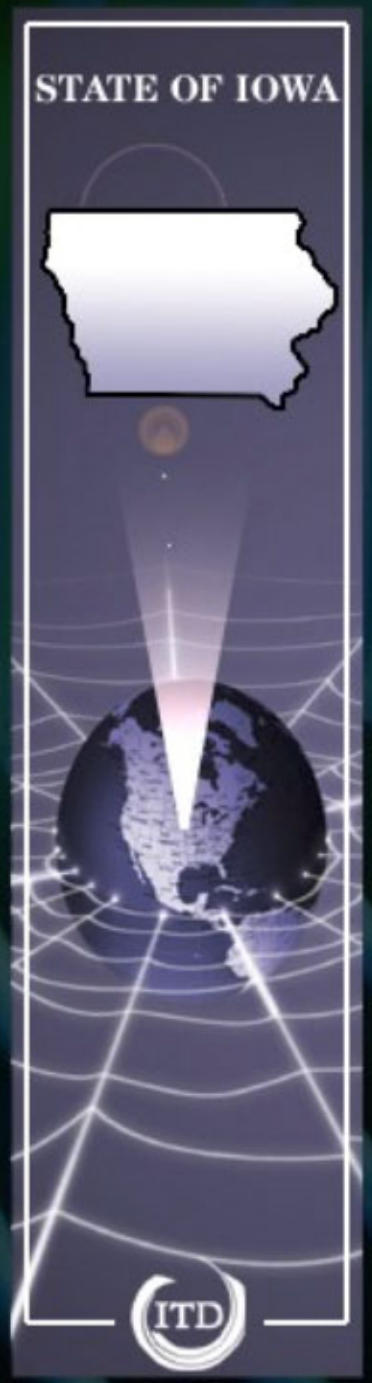
Malicious Code

- All Workstations must have Virus Protection
- Always Scan New Files and Disks for Viruses
- Do not trust unsolicited e-mail attachments



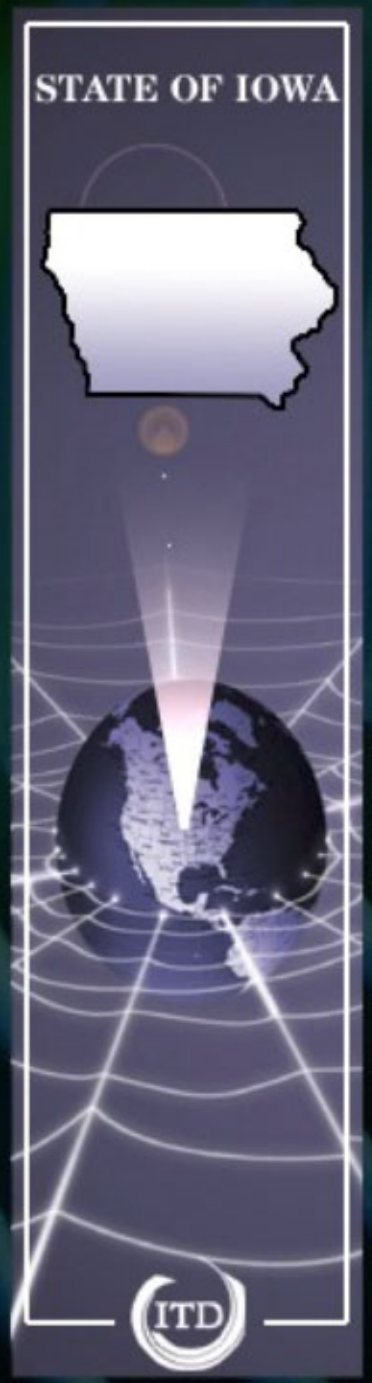
Software Restrictions

- Need authorization before installing any software
- Do not install unlicensed, unapproved software



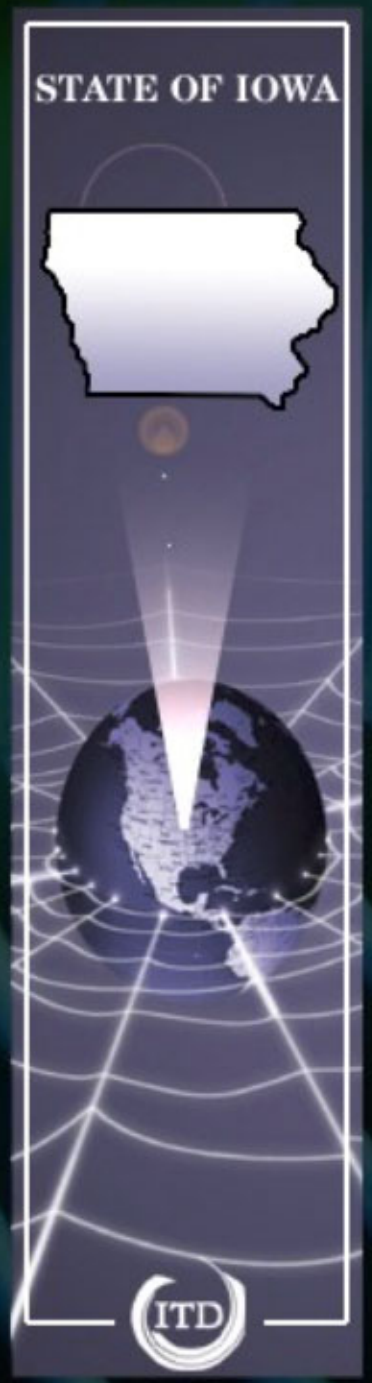
Modems

- Only authorized modems allowed
- Never connect to both an ISP and the State Network simultaneously
- Turn auto-answer OFF



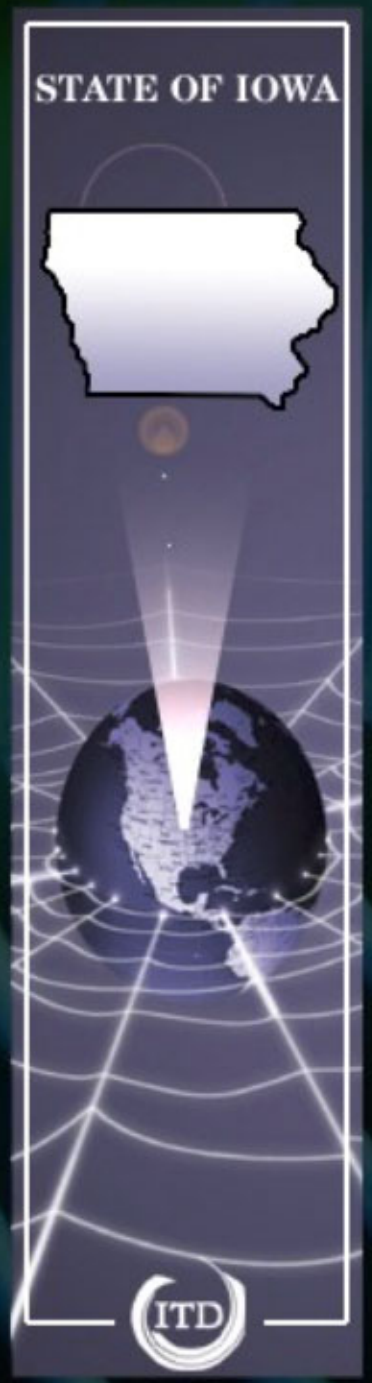
Behavior

- Security Awareness + Proactive Behavior = More Secure Systems
- Small behavior changes can greatly reduce potential for compromise



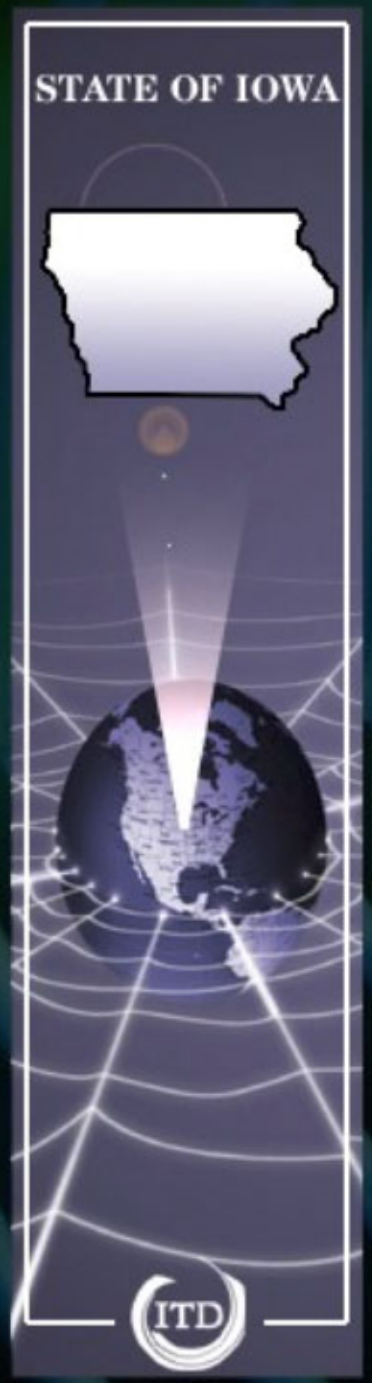
Threats in Code

- Buffer Overruns
- Race Conditions
- Unauthorized Access



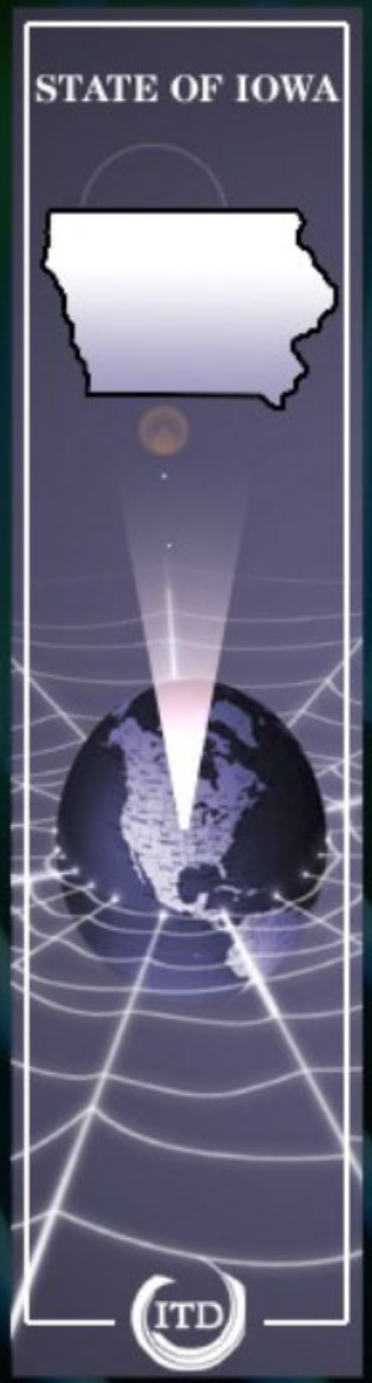
Design Issues

- Secure Authentication
- Data Validation
- User Session Security



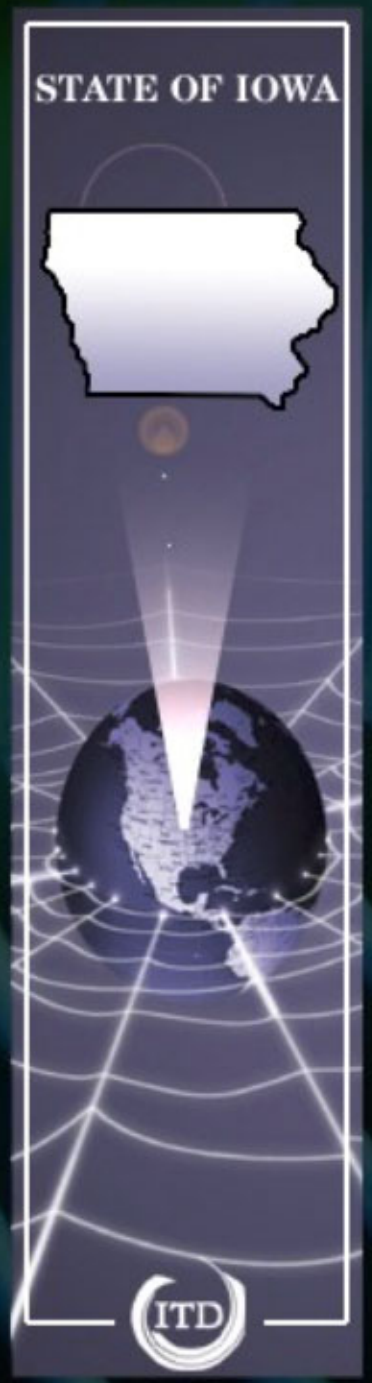
Six Steps to follow

- 1) Focus on authentication and authorization
- 2) Don’t trust user input



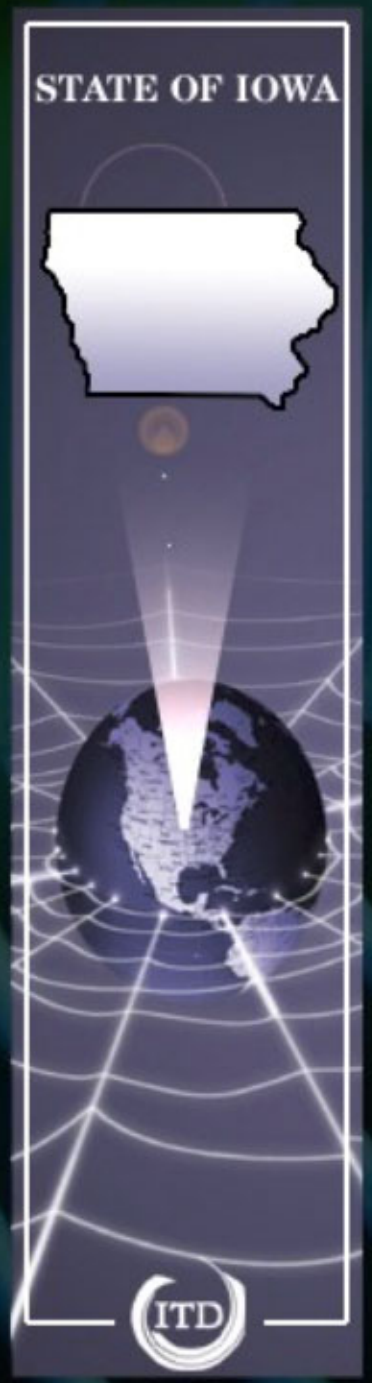
Six Steps cont…

- 3) End-to-end session encryption
- 4) Safe data handling



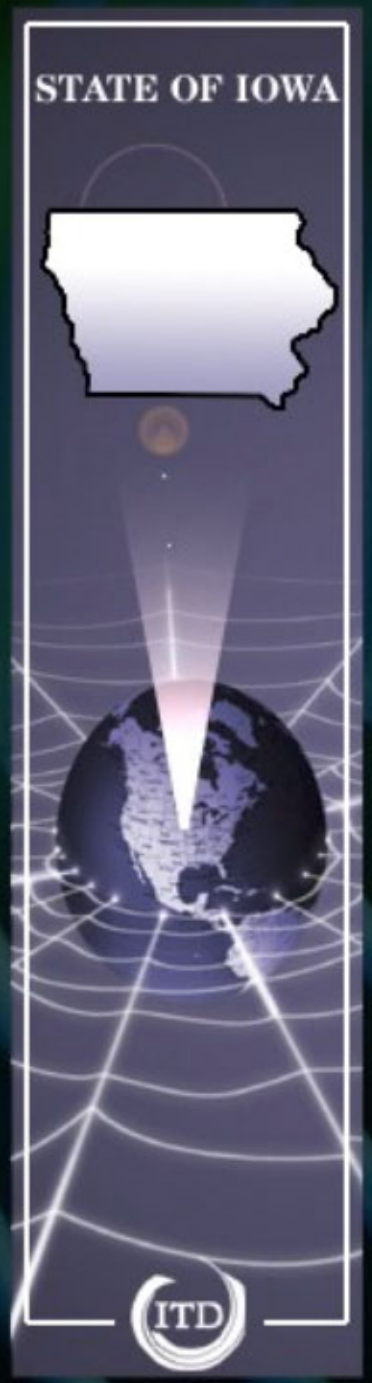
Six Steps cont…

- 5) Eliminate default settings and administrator backdoors
- 6) Quality assurance



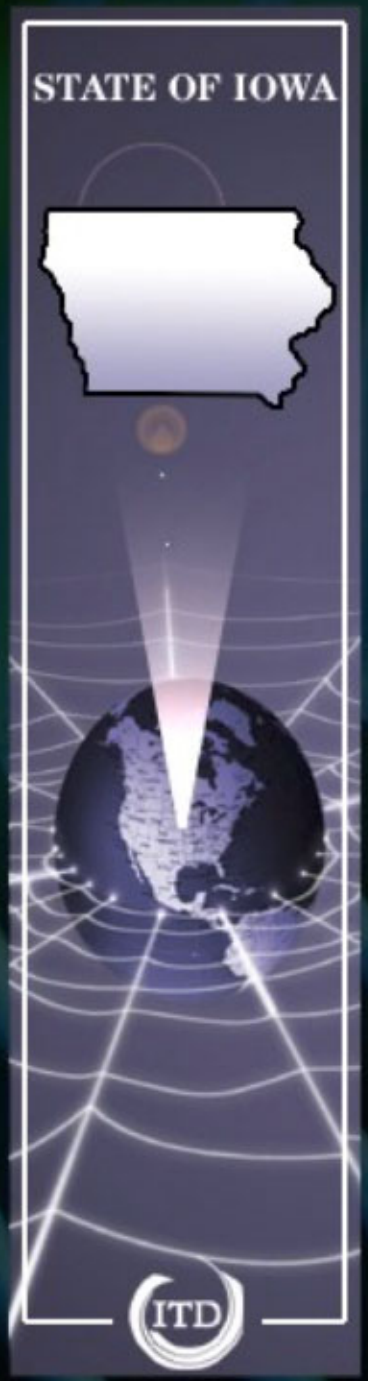
Plan of Action

- Don’t depend on the firewall
- Educate developers
- Build an auditing process into the lifecycle



Summary

- Good security starts in design methodology
- Treat users as hostile attackers
- Research known programming flaws



Links

- **Secure Programming for Linux and Unix**
- *This link has great* ***tips for web programming and helpful hints for specific language issues***
- http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/index.html

- **Multiple Links to secure coding web sites**
- http://www.shmoo.com/securecode/

- **Good article by @Stake application security**
- http://www.vnunet.com/News/1129340

- **Brief guide on insecurities in different languages**
- http://archive.ncsa.uiuc.edu/General/Grid/ACES/security/programming/